NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapt
Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Ch
Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapt
Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

Chapter 7 System Characterization, Information Categorization, System Types, and System Boundaries

7.1 System Characterization

7.1.1 The characterization of a system is based on: the categorization of its information and impact level, the designation of the system type, and identification of its system boundaries. The activity of characterizing the system can sometimes be a lengthy process as different requirements are sorted out.

7.1.2 All three elements in the system characterization process should be considered together. These characteristics will determine the system security controls.

7.2 Categorization of Information

7.2.1 To determine the potential impact to an information system and the level of security required to manage risk to an acceptable level, the information itself must be analyzed for its three IT security objectives and the impact each would have on the mission or functional line of business. The result of the analysis is an "IT security category." The methodology for the categorization of information is documented in the FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems. The security objectives are defined as:

a. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

b. Integrity. Guarding against unauthorized information modification or destruction, which includes ensuring information non-repudiation and authenticity. Loss of integrity is the

unauthorized modification or destruction of information.

c. Availability. Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

7.2.2 For each security objective there are levels of potential impact which must be considered. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or availability of the information or information system would have on NASA operations, including mission, functions, image, or reputation, NASA assets, or individuals (including privacy considerations). The potential impact analysis should focus on the risk to the mission or functional line of business. (See FIPS 199, Table 1 for a detailed explanation of potential impacts for confidentiality, integrity, and availability). The levels of potential impact are:

a. Low. The potential impact is considered low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on NASA operations, organizational assets, or individuals.

b. Moderate. The potential impact is considered moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on NASA operations, organizational assets, or individuals.

c. High. The potential impact is considered high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on NASA operations, organizational assets, or individuals.

d. Not applicable. The potential impact is considered not applicable if the loss of confidentiality has no impact (because the information is already in the public domain). Integrity and availability are never considered not applicable.

7.2.3 An information system may be intended to process, handle, or store many types of information such as privacy information, budget information, research data, public affairs information, capital planning, inventory data, and human resource information. Each type of information shall be analyzed for the potential impact to its confidentiality, integrity, and availability. Establishing an appropriate security category for an information type requires determining the potential impact for each security objective associated with the particular information type. The generalized format for expressing the security category of an information type is shown in Figure 7-1.

SECURITY CATEGORY information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}

Figure 7-1 Security Category Expression

7.2.4 For any information system, the impact values assigned to the information system will be the highest value of the respective security objectives of confidentiality, integrity, availability. The "high water mark" will be selected from the security categories that have been determined for each type of information resident on the information system.

7.2.5 Acceptable values for the potential impact are low, moderate, or high. In the case of confidentiality, not applicable is an acceptable value for information that is available to the public already.

7.3 Categorization of Information Requirements

7.3.1 NASA shall follow the guidance in FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, for the categorization of information.

7.3.2 The SSP for a master system shall:

a. Identify the major information types, which will be processed, handled, or stored.

b. Document the highest impact value (i.e., low, moderate, high) for each IT security objective as the IT security category.

c. Justify any management determination that a different security category is more appropriate than the one recommended by NIST SP 800-60, Volume I and II, Guide for Mapping Types of Information and Information to Security Categories.

7.3.3 The SSP for subordinate systems shall:

a. Document the associated master system's determination of the IT security category and impact value, which are inherited by the subordinate system.

b. Provide justification for any site-specific, information system owner determination that a different category is more appropriate than the one recommended by the master SSP, either higher or lower.

c. Identify the result in the Accreditation Package.

d. Document the concurrence or non-concurrence of the Center CIO and the ITSM on the certification security assessment report.

7.4 Information Technology System Types

7.4.1 The NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, will assist in understanding the relationship between categorization and system types. The OMB Circular A-130, Appendix III requires that Federal information systems be categorized into two types of systems, major applications (MA) and general support systems (GSS). Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. In NPR 1600.1, NASA Security Program Procedural Requirements, 8.4, NASA Critical Infrastructure and Key Resources, NASA has elected to designate its critical infrastructure and key resources as Mission Essential Infrastructure (MEI) to better facilitate designation of vital "mission-oriented" critical infrastructure and key resources.

7.4.1.1 Major Application (MA). An MA system is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of, the information in the application. A breach in an MA has the potential to compromise many individual application programs and hardware, software, and telecommunications components. MA systems can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

7.4.1.2 General Support System (GSS). A GSS system is an interconnected information resource under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, facilities, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

7.4.1.3 NASA Critical Infrastructure and Key Resources--MEI Protection Program. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, directs agencies to establish a program to identify critical infrastructure and key

resources, evaluate these assets for vulnerabilities, and fund and implement appropriate security enhancements (procedural and physical) to mitigate vulnerabilities. NASA has elected to designate its critical infrastructure and key resources as MEI to better facilitate designation of vital "mission oriented" critical infrastructure and key resources.

7.4.2 Information Technology System Types Requirements

7.4.2.1 All master system and subordinate owners shall work with their Center or Agency ITSM(s) to determine whether their master system or subordinate system is either a GSS or MA, as referenced in Guide for Developing Security Plans for IT Systems NIST SP 800-18, Guide for Developing Security Plans for IT Systems. Master and subordinate systems are addressed in Chapter 8, Master and Subordinate IT Systems.

7.4.2.2 Master systems shall be identified as either an MA system or a GSS. A Master, or "umbrella," system is one which provides an overall picture of the security of the systems under an Agency Deputy Mission Director's responsibility and is a key component of the certification and accreditation process. Master systems are supported by subordinate SSPs for individual systems.

7.4.2.3 Subordinate systems shall have the same IT system type (MA or GSS) as the associated master system. Subordinate systems support a master system. Certification testing of security controls is to be accomplished at the subordinate system level.

7.4.2.4 MEI systems shall be master systems identified as an MA or a GSS system.

7.5 System Boundaries

7.5.1 A system is defined by logical boundaries placed around a set of IT processes, communications, storage, and related resources, as well as any interdependence on other systems. The elements within these boundaries constitute a single system requiring a security plan. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems and NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems provide additional guidance. Assigning resources to an information system defines the security accreditation boundary for that system. C&A is required of all IT resources within the boundary and the security posture of any interdependencies identified, verified, and documented. The following factors (described in Chapter 6, Information and Information System IT Security Strategy, Section 7.2, Categorization of Information, Section 7.3, Categorization of Information Requirements, and Chapter 8, Master and Subordinate IT Systems) shall be considered in assigning the system boundary: the categorization of information, the information system type, the assignment as a master or subordinate system, and the system's IT security strategy.

7.5.2 System Boundaries Requirements

7.5.2.1 IT system boundaries shall encompass IT resources:

a. Which are all under the same higher management authority.

b. Which perform the same mission or functional line of business.

c. Which have essentially the same operating characteristics and IT security category.

d. Which are interconnected or networked.

e. Which reside in the same general operating environment or in various locations with similar operating environments.

7.5.2.2 System boundaries shall be:

a. Defined and documented in the SSP for both master and subordinate systems.

b. Established prior to conducting the initial risk assessment.

c. Negotiated among the information system owner, the AO, the cognizant CIO, and the IAO.

7.5.2.3 Master system boundaries shall:

a. Have the same information security category for all systems under its accreditation authority.

b. Be coordinated with the OCIO to ensure the security accreditation boundary supports the NASA Enterprise Architecture.

c. Be subdivided into subordinate systems when the resources are large or complex or have dispersed local operational and security management.

7.5.2.4 Once the initial boundaries have been determined, the information system owner shall review Chapter 6, Information and Information System IT Security Strategy, to ensure that the system is still in line with the information and IT information system security strategy.

7.6 Additional System Characterization, Information Categorization, System Types, and System Boundaries References

a. OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources.

b. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

c. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook.

d. NIST SP 800-18, Guide for Developing Security Plans for IT Systems.

e. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

f. NIST SP 800-60, Volumes I and II, Guide for Mapping Types of Information and Information Systems to Security Categorization Levels.

g. NPR 1600.1, NASA Security Program Procedure Requirements.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapt
Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter
Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17
| Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB
AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS